Oracle® Communications LSMS

Security Guide

Release 13.0

E52613 Revision 2

December 2014

ORACLE®

Oracle® Communications Security Guide, Release 13.0

Table of Contents

List of Tables

Chapter 1

Introduction

Topics:

This chapter contains general information such as an overview of the manual, how to get technical assistance, and where to find additional information.

Overview

This manual describes how to ensure a secure installation of Oracle Communications LSMS (LSMS), and explains LSMS security features.

Scope and Audience

This manual is intended for system administrators that are installing and configuring LSMS.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
	**Danger**: (This icon and text indicate the possibility of *personal injury*.)
	**Warning**: (This icon and text indicate the possibility of *equipment damage*.)
	**Caution**: (This icon and text indicate the possibility of *service interruption*.)
	**Topple**: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Manual Organization

This manual contains the following chapters:

- *Introduction* contains general information such as an overview of the manual, how to get technical assistance, and where to find more information.
- *LSMS Security Overview* describes basic security considerations and provides an overview of LSMS security.
- *Performing a Secure LSMS Installation* describes the process to ensure a secure installation of LSMS.
- *Implementing LSMS Security* explains LSMS security features.
- *Secure Turnover to Customer* describes the secure password turnover process used to ensure security of systems delivered to our customers.

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions

- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See *Locate Product Documentation on the Oracle Technology Network Site* for more information.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Select the **Applications** tile.
   The **Applications Documentation** page appears.
3. Select **Apps A-Z**.
4. After the page refreshes, select the **Communications** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **View** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **PDF** link and select **Save Target As**.

Chapter 2

LSMS Security Overview

Topics:

This chapter describes basic security considerations and provides an overview of LSMS security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See *Performing a Secure LSMS Installation* for more information.
- **Learn about and use the LSMS security features.** See *Implementing LSMS Security* for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site:*http://www.oracle.com/technetwork/topics/security/alerts-086861.html*

Understanding the LSMS Environment

When planning your LSMS implementation, consider the following questions:

- Which resources need to be protected?
  - You need to protect customer data, such as telephone number (TN) information and associated data.
  - You need to protect internal data, such as proprietary source code.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting data from?

  For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your work flows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- What happens if protections on strategic resources fail?

  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Overview of LSMS Security

The LSMS is a secure and reliable Local Number Portability (LNP) system that enables customers to administer their LNP data in a central place.

Operating System Security

Oracle Communications Tekelec Platform (TPD) handles all operating system security for the LSMS application. Make sure you always have the latest TPD software/patches installed on your machines.

TMN Toolkit licenses must be installed for both LSMS servers. License files are obtained from NE Technologies, Inc. For information about how to obtain and install the TMN Toolkit licenses, refer to the LSMS 13.0 *Upgrade/Installation Procedure*.

Database Security

The following LSMS-specific security considerations apply to the MySQL database:

- Secure Database Access Credentials

  Only authorized personnel are allowed to access the database and a user ID and password are required.

  Provide minimum privileges to the user so that unauthorized modifications can be avoided. For more information, see *Managing User Accounts*.

- Use SSH/SSL Connections

  SSH/SSL is a robust, commercial-grade, and full-featured toolkit that implements the security and network encryption. SSH/SSL provides secure data transmission through encryption keys.

  Encryption is required for the connection between the NPAC and the LSMS. The LSMS has a key for each NPAC that it services. For more information about using key lists, refer to the *Configuration Guide*.

- Modify the MySQL Port for Query Servers

  Since the default MySQL port 3306 is a well-known port, to prevent eavesdropping use the LSMS GUI to change the MySQL port for query servers. For more information about modifying the MySQL port for query servers, see the *Alarms and Maintenance Guide*.

SPID Security for Locally Provisioned Data

Without the optional Service Provider Identifier (SPID) Security feature, any user is able to log in using any SPID that is defined on the LSMS. The user is able to view any data for any SPID, and depending on the user privileges that were assigned to the user, the user might even be able to change data associated with any SPID.

The SPID Security feature enables the LSMS administrator to control the users that can log on with a specified SPID. In addition, the LSMS administrator can assign special access to a user that provides access to all SPIDs; such a user is called a *golden user*.

The SPID Security feature is especially useful for LSMS customers that act as service bureaus, offering LSMS services to other service providers. The service bureau may administer locally provisioned data

for a client and may choose to allow the client to administer or view its own data without allowing that client to view or change data belonging to other clients.

For more information, refer to *Managing SPID Security*.

Chapter 3

Performing a Secure LSMS Installation

Topics:

This chapter describes the process to ensure a secure installation of LSMS.

Pre-Installation Configuration

All pre-installation configuration is set by TPD. No additional user configuration regarding security is required.

Installing LSMS Securely

The standard TPD installation process, *Initial Product Manufacture* (IPM) 5.0+, ensures a secure installation of the LSMS application. All non-essential and non-secure services are removed or excluded from the default installation.

Oracle recommends using the default installation, unless there are specific customer needs for additional services.

Post-Installation Configuration

There are no required post-installation configuration changes pertaining to Security.

Establishing various network connections from the LSMS to other customer network elements is performed by using the LSMS GUI as documented in the *Configuration Guide*.

Chapter 4

Implementing LSMS Security

Topics:

This chapter explains the LSMS security features.

Managing User Accounts

The system administrator assigns user names and passwords, and each user name is assigned to one of the following permission groups:

- lsmsall
- lsmsadm
- lsmsuser
- lsmsuext
- lsmsview

The permission groups govern which commands and which GUI functions the user is allowed to use.

Note: It is possible for an individual user name to have the same value as a group name. For example, usually a user named lsmsadm is assigned to the lsmsadm permission group. Some LSMS commands require the user to be logged in with the lsmsadm user name.

For more information about managing user accounts, refer to the *Alarms and Maintenance Guide*.

Managing Password Security

By default, the LSMS does not provide any password expiration limit. The password expiration limit must be set by the system administrator using the LSMS GUI or the command line interface utility (lsmsclaa).

You can set the limit for password expiration from 1-180 days. After a password expires, the user cannot log in without changing the password.

For more information about setting password timeout values, refer to the *Alarms and Maintenance Guide*.

Managing SPID Security

Association of a user name with a SPID enables the LSMS system administrator to restrict access to the following types of locally provisioned data:

- Default global title translation (GTT)
- Override GTT
- GTT groups
- Telephone number (TN) filters
- Assignment of GTT groups and TN filters to an element management system (EMS)

Accessibility to these types of data is protected by SPID Security for any access method (for example, through the GUI, or through input data by file, audit, and reconcile).

The optional SPID Security feature is activated by Oracle customer service using secure activation procedures. After the feature is activated, the LSMS system administrator is advised to immediately

define associations between user names and SPIDs. For information about associating user names with SPIDs, refer to the *Alarms and Maintenance Guide*.

Modifying the MySQL Port

This optional feature enhances the security of LSMS databases by enabling the system administrator to change the MySQL port. By default, MySQL uses port 3306, and because this is a well-known port you should change it.

Through the LSMS GUI, the MySQL port can be configured to ports 34000-34099. The port can be maintained through the GUI, and any changes to the port setting will raise an alarm on the LSMS. The MySQL port can also be changed back to the default port if necessary.

For information about how to modify the MySQL port, refer to the *Alarms and Maintenance Guide*.

Using Login Sessions

You can log into the LSMS command line or the LSMS GUI to configure and maintain the LSMS system.

- You can access the command line from any terminal that has the Secure Shell (ssh) client installed.

  If your terminal does not already have ssh installed, PuTTY (Oracle does not make any representations or warranties about this product) is an open source ssh utility for Windows that you can download from the web.

- You can access the GUI through a web browser if you activate the optional IP User Interface feature.

  If you have not activated the IP User Interface feature, you can establish a login session first from an X-windows compatible terminal and then start a GUI session.

You must have a user ID and password before you can log in to LSMS.

For more information about using login sessions, refer to the *Alarms and Maintenance Guide*.

Appendix A

Secure Turnover to Customer

Topics:

To ensure security of systems delivered to our customers and to satisfy Oracle policies, all passwords must be owned by the customer once transfer of ownership of systems has occurred.

Secure Turnover Process

Three key requirements address the fundamental principles of the secure turnover process:

- Oracle default passwords shall not remain on fielded systems.
- Oracle default passwords shall not be revealed to customers.
- Customer installed passwords shall not be known by Oracle.

Goals of the Secure Turnover Process

Following are the goals of the password handoff process:

1. Install the system securely with Oracle internal default passwords (passwords exclusively known and used by Oracle personnel).
2. Change the special account passwords during the installation process to a unique value (meeting password complexity rules required by the system).
3. Provide a non-repudiation process for the customer agent to set all special passwords.

Secure Turnover Procedure

Perform the following steps for secure system turnover:

1. System servers are installed by Oracle personnel using common ISO deliverables and installation procedures. The OS root password, OS admusr password, and the passwords for the default LSMS login accounts (lsmsadm, lsmsmgr, and platcfg) are from the build process, and are private and known only by Oracle.
2. Following installation, the Oracle installer performs a login to each server OS (real and virtual) as admusr and changes the password to a new unique secure password. The Oracle installer then switches user to root and changes the root password to a new unique password.
3. The Oracle installer uses a web browser to log in to the application on each relevant server using each default LSMS login name (such as lsmsadm) and changes the password to a new unique password.
4. As a precursor to the official handoff of the system (all servers) to the customer, the Oracle installer ensures that the new unique passwords for root, admusr, and default LSMS login accounts have been securely given to the authorized customer agent.
5. The authorized customer agent is instructed to log in to each OS account on each server (real and virtual) and change the password for accounts admusr and root to the authorized operational setting for the customer.

6. The customer agent is instructed to use a web browser to log in to each relevant application server and change the password for the default LSMS login accounts to the authorized operational password for the customer.
7. Following the entry of the new passwords by the customer agent, the Oracle installer or authorized Oracle agent attempts to log in to each server using the previously known password. This should result in a failed login attempt verifiable in the server logs.
8. The customer agent again logs in to each OS account and the default LSMS login accounts using the new customer passwords to verify success with the new customer passwords.

Glossary

G

GUI

Graphical User Interface

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

L

LSMS

Local Service Management System

An interface between the Number Portability Administration Center (NPAC) and the LNP service databases. The LSMS receives LNP data from the NPAC and downloads that data to the service databases. LNP data can be entered into the LSMS database. The data can then be downloaded to the LNP service databases and to the NPAC.